THAT WHICH IS CLAIMED IS:

1. A method of generating an RSA cryptographic value, the method comprising the steps of:

obtaining user specific information about a user; and

dividing the potential range of RSA prime values into at least two subintervals;

selecting a first user-dependent RSA prime from a range of RSA prime values in a first of the at least two subintervals corresponding to a user specific range of values based on the user specific information mapped onto the first subinterval.

2. A method according to Claim 1, further comprising the steps of:

selecting a second user-dependent RSA prime from a range of RSA prime values in a second of the at least two subintervals, different from the first subinterval, corresponding to the user specific range of values based on the user specific information mapped onto the second subinterval.

3. A method according to Claim 1, wherein the user specific range of values are mapped by linearly mapping the user specific range of values onto the first subinterval.

4. A method according to Claim 2, wherein the user specific range of values are mapped onto the first subinterval and mapped onto the second subinterval utilizing the same mapping function.

5. A method according to Claim 2, further comprising the step of generating a user-dependent RSA key value from the first and second user-dependent primes.

6. A method according to Claim 1, wherein the RSA prime values comprise n bits and wherein the first subinterval comprises RSA prime values from the set $[\sqrt{2}(2^{n-1}), 2^{n-1}+2^{n-3/2}]$ and the second subinterval comprises RSA prime values from the set $[2^{n-1}+2^{n-3/2}, 2^n]$.

7. A method according to claim 2, wherein the RSA prime values comprise n bits and wherein the difference between the first RSA prime and the second RSA prime is greater than 2^{n-2}.

8. A method according to Claim 3, wherein the first subinterval comprises an interval [a,b], wherein the user specific range comprises an interval [c,d] and wherein the linear mapping function comprises the function defined by,

$$F(x) = ux + v \text{ , where } u = \frac{d-c}{b-a} \text{ and } v = \frac{bc-ad}{b-a} .$$

9. A method according to Claim 1 further comprising the step of selecting a second RSA prime from the potential range of RSA prime values.

10. A method according to Claim 1, wherein the user specific information is biometric information.

a^2 cont

11. A method according to Claim 1, wherein the user specific information is a globally unique user identification.

12. A method according to Claim 1, wherein the step of selecting a first user-dependent RSA prime comprises the steps of:

selecting a random point in the range of RSA prime values in the first subinterval corresponding to the mapped user specific range of values;

utilizing the random point as a starting point for a search for a prime number (p) in the range of RSA prime values in the first subinterval corresponding to the mapped user specific range of values.

13. A method according to Claim 12, further comprising the steps of:

determining if a candidate for p is considered outside the range of RSA prime values in the first subinterval corresponding to the mapped user specific range of values;

selecting a new random point as a search starting point if a candidate for p is considered outside the range of RSA prime values in the first subinterval

corresponding to the mapped user specific range of values; and

restarting the search for p utilizing the new random point.

14. A system for generating an RSA cryptographic value, comprising:

means for obtaining user specific information about a user; and

means for determining a user specific range of values based on the user specific information;

means for dividing the potential range of RSA prime values into at least two subintervals;

means for mapping the user specific range of values onto a first of the at least two subintervals; and

means for selecting a first user-dependent RSA prime from the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values.

15. A system according to Claim 14, further comprising:

means for mapping the user specific range of values onto a second of the at least two subintervals, different from the first of the at least two subintervals;

means for selecting a second user-dependent RSA prime from the range of RSA prime values in the second of the at least two subintervals corresponding to the mapped user specific range of values.

16. A system according to Claim 15, wherein the means for mapping comprises means for linearly mapping the user specific range of values onto a first of the at least two subintervals.

17. A system according to Claim 16, wherein the means for mapping the user specific range of values onto a first of the at least two subintervals and the means for mapping the user specific range of values onto a second of the at least two subintervals, different from the first of the at least two subintervals utilize the same mapping function.

Q2 cont

18. A system according to Claim 15, further comprising means for generating a user-dependent RSA key value from the first and second user-dependent primes.

19. A system according to Claim 14, wherein the RSA prime values comprise n bits and wherein the first subinterval comprises RSA prime values from the set $[\sqrt{2}(2^{n-1}), 2^{n-1}+2^{n-3/2}]$ and the second subinterval comprises RSA prime values from the set $[2^{n-1}+2^{n-3/2}, 2^n]$.

20. A system according to claim 15, wherein the RSA prime values comprise n bits and wherein the

difference between the first RSA prime and the second RSA prime is greater than 2^{n-2}.

21. A system according to Claim 16, wherein the first subinterval comprises an interval [a,b], wherein the user specific range comprises an interval [c,d] and wherein the linear mapping function comprises the function defined by,

$$F(x) = ux + v, \text{ where } u = \frac{d-c}{b-a} \text{ and } v = \frac{bc-ad}{b-a}.$$

22. A system according to Claim 14 further comprising means for selecting a second RSA prime from the potential range of RSA prime values.

23. A system according to Claim 14, wherein the user specific information is biometric information.

24. A system according to Claim 14, wherein the user specific information is a globally unique user identification.

25. A system according to Claim 14, wherein the means for selecting a first user-dependent RSA prime comprises:

means for selecting a random point in the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values;

means for utilizing the random point as a starting point for a search for a prime number (p) in the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values.

26. A system according to Claim 25, further comprising:

means for determining if a candidate for p is considered outside the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values;

means for selecting a new random point as a search starting point if a candidate for p is considered outside the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values; and

means for restarting the search for p utilizing the new random point.

27. A computer program product for generating an RSA cryptographic value, comprising:

a computer readable storage medium having computer readable program code means embodied in said medium, said computer readable program code means comprising:

computer-readable program code means for obtaining user specific information about a user; and

computer-readable program code means for determining a user specific range of values based on the user specific information;

computer-readable program code means for dividing the potential range of RSA prime values into at least two subintervals;

computer-readable program code means for mapping the user specific range of values onto a first of the at least two subintervals; and

computer-readable program code means for selecting a first user-dependent RSA prime from the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values.

28. A computer program product according to Claim 27, further comprising:

computer-readable program code means for mapping the user specific range of values onto a second of the at least two subintervals, different from the first of the at least two subintervals;

computer-readable program code means for selecting a second user-dependent RSA prime from the range of RSA prime values in the second of the at least two subintervals corresponding to the mapped user specific range of values.

29. A computer program product according to Claim 28, wherein the computer-readable program code means for mapping comprises computer-readable program code means for linearly mapping the user specific range of values onto a first of the at least two subintervals.

30. A computer program product according to Claim 29, wherein the computer-readable program code means for mapping the user specific range of values onto a first of the at least two subintervals and the computer-readable program code means for mapping the user specific range of values onto a second of the at least two subintervals, different from the first of the at least two subintervals utilize the same mapping function.

Q2 cont

31. A computer program product according to Claim 28, further comprising computer readable code means for generating a user-dependent RSA key value from the first and second user-dependent primes.

32. A computer program product according to Claim 26, wherein the RSA prime values comprise n bits and wherein the first subinterval comprises RSA prime values from the set $[\sqrt{2}(2^{n-1}), 2^{n-1}+2^{n-3/2}]$ and the second subinterval comprises RSA prime values from the set $[2^{n-1}+2^{n-3/2}, 2^n]$.

33. A computer program product according to claim 28, wherein the RSA prime values comprise n bits and wherein the difference between the first RSA prime and the second RSA prime is greater than 2^{n-2}.

34. A computer program product according to Claim 29, wherein the first subinterval comprises an interval [a,b], wherein the user specific range comprises an interval [c,d] and wherein the linear mapping function comprises the function defined by,

$$F(x)=ux+v \text{ , where } u=\frac{d-c}{b-a} \text{ and } v=\frac{bc-ad}{b-a} .$$

a^2 con't

35. A computer program product according to Claim 27 further comprising computer-readable program code means for selecting a second RSA prime from the potential range of RSA prime values.

36. A computer program product according to Claim 27, wherein the user specific information is biometric information.

37. A computer program product according to Claim 27, wherein the user specific information is a globally unique user identification.

38. A computer program product according to Claim 27, wherein the computer-readable program code means for selecting a first user-dependent RSA prime comprises:

computer-readable program code means for selecting a random point in the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values;

computer-readable program code means for utilizing the random point as a starting point for a search for a prime number (p) in the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values.

39. A computer program product according to Claim 38, further comprising:

computer-readable program code means for determining if a candidate for p is considered outside the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values;

computer-readable program code means for selecting a new random point as a search starting point if a candidate for p is considered outside the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values; and

computer-readable program code means for restarting the search for p utilizing the new random point.

40. A method of generating a cryptographic value corresponding to a source entity, the method comprising the steps of:

obtaining entity specific information associated with the source entity;

selecting a cryptographic value from a range of cryptographic values based on the entity specific

information, wherein the range of cryptographic values based on the entity specific information is disjoint with ranges of cryptographic values associated with entity specific information associated with entities other than the source entity.

41. A method according to Claim 40, wherein the entity specific information comprises biometric information associated with a user.

42. A method according to Claim 40, wherein the entity specific information comprises a globally unique user identification associated with a user.

43. A method according to Claim 40, wherein the entity specific information comprises a company identification.

44. A method according to Claim 40, wherein the cryptographic value comprises an RSA key and wherein the step of selecting comprises selecting the RSA key from a portion of the range of potential RSA key values based on the entity specific information, wherein portion of the range of potential RSA key values is defined by mapping an entity specific range of values onto the range of potential key values.

45. A method according to Claim 40, further comprising the step of authenticating the source entity of the cryptographic value by determining if the cryptographic value is within the range of

cryptographic values based on the entity specific information associated with the source entity.

46. A system for generating a cryptographic value corresponding to a source entity, comprising:

means for obtaining entity specific information associated with the source entity;

means for selecting a cryptographic value from a range of cryptographic values based on the entity specific information, wherein the range of cryptographic values based on the entity specific information is disjoint with ranges of cryptographic values associated with entity specific information associated with entities other than the source entity.

47. A system according to Claim 46, wherein the entity specific information comprises biometric information associated with a user.

48. A system according to Claim 46, wherein the entity specific information comprises a globally unique user identification associated with a user.

49. A system according to Claim 46, wherein the entity specific information comprises a company identification.

50. A system according to Claim 46, wherein the cryptographic value comprises an RSA key and wherein the means for selecting comprises means for selecting

the RSA key from a portion of the range of potential RSA key values based on the entity specific information, wherein portion of the range of potential RSA key values is defined by mapping an entity specific range of values onto the range of potential key values.

51. A system according to Claim 46, further comprising means for authenticating the source entity of the cryptographic value by determining if the cryptographic value is within the range of cryptographic values based on the entity specific information associated with the source entity.

52. A computer program product for generating a cryptographic value corresponding to a source entity, comprising:

a computer readable storage medium having computer readable program code means embodied in said medium, said computer readable program code means comprising:

computer readable program code means for obtaining entity specific information associated with the source entity;

computer readable program code means for selecting a cryptographic value from a range of cryptographic values based on the entity specific information, wherein the range of cryptographic values based on the entity specific information is disjoint with ranges of cryptographic values associated with entity specific information associated with entities other than the source entity.

53. A computer program product according to Claim 52, wherein the entity specific information comprises biometric information associated with a user.

54. A computer program product according to Claim 52, wherein the entity specific information comprises a globally unique user identification associated with a user.

Q2 cont

55. A computer program product according to Claim 52, wherein the entity specific information comprises a company identification.

56. A computer program product according to Claim 52, wherein the cryptographic value comprises an RSA key and wherein the computer readable program code means for selecting comprises computer readable program code means for selecting the RSA key from a portion of the range of potential RSA key values based on the entity specific information, wherein portion of the range of potential RSA key values is defined by mapping an entity specific range of values onto the range of potential key values.

57. A computer program product according to Claim 52, further comprising computer readable program code means for authenticating the source entity of the cryptographic value by determining if the cryptographic value is within the range of cryptographic values based on the entity specific information associated with the source entity.